ABSTRACT

In general, one embodiment of the invention features a method comprising operations performed internally within a device. A first operation involves generating data for permanent storage in a protected area of internal memory of the device. This prevents subsequent modification of the data. A second operation involves producing a secret value being a combination of both the data and a short term value generated in response to a periodic event such as a power-up sequence of a platform employing the device.